ode: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 211115-0232]

Announcing Issuance of Federal Information Processing Standard (FIPS) 201-3, Personal Identity Verification (PIV) of Federal Employees and Contractors

AGENCY: National Institute of Standards and Technology (NIST), Commerce.

ACTION: Notice.

SUMMARY: This notice announces the Secretary of Commerce's approval of Federal Information Processing Standard (FIPS) Publication 201-3, Personal Identity Verification (PIV) of Federal Employees and Contractors. FIPS 201-3 includes clarifications to existing text, additional text in cases where there were ambiguities, adaptation to changes in the environment since the publication of FIPS 201-2, and specific changes requested by Federal agencies and implementers.

DATES: FIPS 201-3 is effective on **[INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: FIPS 201-3 is available electronically from the NIST Web site at: https://csrc.nist.gov/publications/fips. Comments that were received on the proposed changes will also be published electronically at https://csrc.nist.gov/projects/piv and at https://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: Hildegard Ferraiolo, (301) 975-6972, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8930, Gaithersburg, MD 20899-8930, email: hildegard.ferraiolo@nist.gov, or Andrew Regenscheid, (301) 975-5155, andrew.regenscheid@nist.gov.

SUPPLEMENTARY INFORMATION:

FIPS 201 establishes a standard for a Personal Identity Verification (PIV) system (Standard) that meets the control and security objectives of Homeland Security Presidential Directive-12 (HSPD-12). It is based on secure and reliable forms of identity credentials issued by the Federal Government to its employees and contractors. These credentials are used by mechanisms that authenticate individuals who require access to federally controlled facilities, information systems, and applications. This Standard addresses requirements for initial identity proofing, infrastructure to support interoperability of identity credentials, and accreditation of organizations issuing PIV credentials.

FIPS 201 was issued on 2005 (70 FR 17975) in response to HSPD-12. Subsequent revisions included FIPS 201-1, published in 2006 and FIPS 201-2 (version in effect), published in 2013 (78 FR 54626). In consideration of technological advancements over the last five years and specific requests for changes from United States Government (USG) stakeholders, NIST determined that a third revision of FIPS 201 was warranted. NIST received numerous change requests, some of which, after analysis and coordination with the Office of Management and Budget (OMB) and USG stakeholders, were incorporated in a proposed draft of FIPS 201-3. Other change requests incorporated in the draft resulted from the 2019 Business Requirements Meeting held at NIST. The meeting focused on business requirements of Federal departments and agencies. On November 3, 2020, a notice was published in the *Federal Register* (85 FR 69599), soliciting public comments on the draft FIPS 201-3. During the public comment period, a virtual public workshop was hosted by NIST on December 9, 2020.

The scope of changes reflected in FIPS 201-3 include the following:

- Alignment with current NIST technical guidelines on identity management, OMB policy guidelines, and changes in commercially-available technologies and services.
- Accommodation of additional types of authenticators through an expanded definition of Derived PIV credentials.
- Focus on the use of federation to facilitate interoperability and interagency trust.

- Addition of supervised remote identity proofing processes.
- Removal of previously deprecated Cardholder Unique Identifier (CHUID) authentication mechanism and deprecation of the symmetric card authentication key and visual authentication mechanisms (VIS).
- Support for secure messaging authentication mechanism (SM-AUTH).

Comments and questions regarding the draft were submitted by USG organizations, private sector organizations, and private individuals. NIST made several changes to the draft FIPS 201-3 based on the public comments received.

Many commenters asked for clarification of the text of the Standard and/or recommended editorial and/or formatting changes. Other commenters suggested modifying the requirements and asked questions concerning the implementation of the Standard. All of the suggestions, questions, and recommendations within the scope of this FIPS were carefully reviewed, and changes were made to the Standard, where appropriate. Some commenters submitted questions or raised issues that were related but outside the scope of this FIPS. Comments that were outside the scope of this FIPS, but that were within the scope of one of the related Special Publications, were deferred for later consideration in the context of the revisions to these Special Publications. The disposition of each comment that was received has been provided along with the comments at https://csrc.nist.gov.

The following is a summary and analysis of the comments received during the public comment period, and NIST's responses to them:

1. Comment: Some commenters inquired about the effective date of the Standard. Commenters also inquired about the implementation schedule associated with the changes introduced in the Standard, once the Standard is in effect.

Response: FIPS 201-3 will be effective immediately upon final publication, superseding FIPS 201-2. The effective date of new and updated features depends upon the release of revised NIST Special Publications or the release of new NIST Special Publications that will be developed

following the publication of this Standard. The implementation schedule may be reflected in NIST's Special Publications or may be provided separately by OMB, as appropriate.

2. Comment: Multiple commenters asked for clarification of the terms PIV account and enrollment records.

Response: New terminology was introduced to define PIV identity account rather than PIV account. The PIV identity account is the cardholder's identity account for PIV credentials including derived PIV credentials. It includes stored or linked contents of enrollment records.

3. Comment: There were multiple commenters who asked for guidance on biometrics and their use in PIV lifecycle processes. The comments related to the type of the biometrics on cards and how long the biometrics were valid.

Response: FIPS 201-3 expands the use of optional biometric modalities (e.g., iris) for issuance and maintenance. The Standard also defines the use of automated facial comparison algorithm as a biometric modality. The Standard maintains the 12-year maximum lifetime for biometrics since studies show that the biometric can be matched for that length of time.

4. Comment: Multiple commenters had concerns about the requirements for validating identity source documents and the requirements for REAL-ID driver's licenses.

Response: NIST emphasized that there are existing requirements to validate identity source documents to be genuine, authentic and unexpired. REAL-ID compliance requirements are clarified by referring to DHS's enforcement guidance.

5. Comment: Commenters had concerns about the supervised remote identity proofing processes introduced in the draft FIPS 201-3. Some commenters sought greater allowances for remote proofing such as unstaffed stations. Clarification was sought on the intended use of the process, requirements for staff at remote sites and the protections applied to remote stations.

Response: The Standard emphasizes the need for a staff to maintain the same level of assurance as in-person processes and to perform sensitive protection and maintenance activities at remote station.

6. Comment: Several commenters requested detailed instructions on reporting card termination.

Response: The Standard was updated to reflect termination in the card management system and in enrollment records.

7. Comment: Several commenters requested changes on the management of derived PIV credentials.

Response: The Standard clarifies processes and terms regarding the issuance or binding of derived PIV credentials to PIV identity accounts. The updates to the Standard include requirements and guidance on re-issuance and post-issuance management of Public Key Infrastructure (PKI) and non-PKI derived PIV credentials.

8. Comment: Some commenters asked that FIPS 201-3 include periodic privacy impact assessments on all PIV related systems.

Response: The Standard was updated to require periodic review of Privacy Impact Assessment.

9. Comment: Several commenters raised concerns related to the requirement for the PIV Card to enforce a blacklist of disallowed PINs. They did not feel the technology was available to enable cards to maintain the blacklist and to provide automated enforcement of selected PINs.

Response: The Standard removed the requirement due to the complexity of enforcing a blacklist by the PIV Card. Instead, the Standard specifies that the card holder be guided to select a strong PIN that is not easily guessable or commonly used.

10. Comment: Some commenters asked to maintain use of the magnetic stripe and not deprecate it in this version of the Standard.

Responses: NIST confirmed the deprecation of the magnetic stripe in this version of the Standard with potential removal in a future revision. Use of the magnetic stripe is still allowed during the deprecation phase but it should begin to be phased out.

11. Comment: Some commenters had concerns on the removal of Legacy PKI. Some commenters asked NIST to clarify how a cross-certified PKI will operate as agencies transition

away from Legacy PKI implementations. Others asked that Legacy PKI use to remain in the Standard.

Response: The Standard was revised to allow departments and agencies that operate their own PKIs to issue digital signature and key management certificates according to agency-specified certificate policies as an alternative to the Federal PKI Common Policy Framework policies referenced by FIPS 201-3. To facilitate greater interoperability and consistency of issuance practices across agencies, the next revision of FIPS 201 will require the use of the specified FPKI policies.

12. Comment: Several commenters asked to either reconsider removal of the CHUID authentication mechanism or clarify the effective date.

Response: The CHUID authentication mechanism was deprecated in the prior revision of the Standard and is designated for removal in this revision. NIST concluded that removal of CHUID authentication is necessary at this time and will become effective when this version of the Standard is approved. OMB will provide additional implementation guidance as necessary.

13. Comment: A few commenters asked that SYM-CAK not be deprecated because it is still supported in some implementations.

Response: Even though SYM-CAK has been deprecated in this version, its use is not prohibited. However, support will be removed in the next revision of the Standard.

14. Comment: Commenters indicated that the Physical Assurance Level (PAL) concept for facility access was not consistent with assurance levels in NIST SP 800-63B.

Response: The Authenticator Assurance Levels (AAL) described in NIST SP 800-63B are specific to network-based authentication, not authentication for facility access. As a result, the final version of the Standard has removed the concept of PAL and disassociated assurance levels from NIST SP 800-63-B for facility access. Instead, authentication mechanisms are described independently from SP 800-63B for facility access.

15. Comment: Multiple commenters expressed concern that the description of assurance levels for logical access at local workstations was not consistent with the AALs defined in NIST SP 800-63B.

Response: The AALs described in NIST SP 800-63B are specified for network-based authentication, not local authentication to workstations. As such, the final version of the Standard describes assurance levels for logical access to local workstations independently from the SP 800-63B-defined AALs.

16. Comment: Several commenters asked for a more detailed description of the operation of Federated IdPs.

Response: IdP terminology was updated to better align with the rest of the document. Secure operation of IdPs will be covered by updates to SP 800-79.

17. Comment: A commenter asked that the use of stable identifiers be included in FIPS 201-3 to support interoperability among federal agencies.

Response: The new Special Publication for Federation, SP 800-217, will describe processes for linking PIV identity accounts to relying party services in interoperable and extensible manners.

18. Comment: A commenter asked that there be a discussion about the direct use and the federated use of PIV credentials.

Response: The Standard explains both the direct and the federated use of PIV credentials. Of the two approaches, the Standard recommends the use of federation protocol as the primary means to accept and process PIV credentials from other agencies.

FIPS 201-3 is available electronically from the NIST Web site at:

https://csrc.nist.gov/publications/fips.

(Authority: 15 U.S.C. 278g-3; HSPD-12.)

Alicia Chambers,

NIST Executive Secretariat.

[FR Doc. 2022-01246 Filed: 1/21/2022 8:45 am; Publication Date: 1/24/2022]